line 7, change "one" to --yet another--;

line 9, change "one" to --an--;

line 11, change "one" to --an--;

line 13, change "one" to --an--;

delete line 15, and insert --DETAILED DESCRIPTION--; and

line 17, change "one" to --an--.

On page 7, line 24, change "one" to --an--.

On page 15, line 27, delete "preferred".

In the Claims:

Please amend the claims as follows:

1. (TWICE AMENDED) A computer readable medium having stored therein a policy file for controlling cryptographic functions of an application program, the computer readable medium comprising:

an attribute portion that **[hold]** holds a plurality of cryptographic policy attributes, each cryptographic policy **[attributes]** attribute representing a cryptographic function;

a value portion that includes a plurality of attribute values, each attribute value corresponding to a separate one of the cryptographic policy attributes and indicating to a policy filter whether an application program may employ the cryptographic policy represented by the attribute; and

a signature portion for verifying authenticity of **[said]** the attribute portion and **[said]** the value portion.

2. (TWICE AMENDED) The medium of claim 1, wherein **[said]** the plurality of cryptographic policy attributes includes cryptographic capabilities of **[said]** the application program in a country where **[said]** the application program is said to be executed.

3. (THREE TIMES AMENDED) The medium of claim 1, wherein each of **[said]** the attribute values is a data string, an integer number, or a truth expression, **[said]** the truth expression including one of a true flag, a false flag, and a conditional flag.

4. (THREE TIMES AMENDED) The medium of claim 1, wherein **[said]** the signature portion includes a digital signature and a chain of certificates, **[wherein said]** the digital signature **[includes]** including a certificate indicative of the origin of **[said]** the digital signature, and **[further, wherein said]** the chain of certificates is indicative of the validity of **[said]** the digital signature.

5. (TWICE AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

storage means for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that store[d]s a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, **[said]** the signature portion including digital certificates for validating a signer's certificate;

control means for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

processing means for selectively processing **[said]** the retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

6. (TWICE AMENDED) The system of claim 5, wherein each of **[said]** the cryptographic policy attributes includes an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression.

7. (TWICE AMENDED) The system of claim 6, wherein **[said]** the truth expression is one of a true flag, a false flag, and a conditional flag.

8. (AMENDED) The system of claim 5, wherein **[said]** the storage means is an archive file.

9. (TWICE AMENDED) The system of claim 5, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage means, and further including decompressing means for decompressing **[said]** the compressed plurality of attributes and values in accordance with said control means retrieving **[said]** the compressed plurality of attributes and values.

10. (TWICE AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

storage means for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stores a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, each of **[said]** the cryptographic policy attributes including an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression, and **[said]** the signature portion including digital certificates for validating a signer's certificate;

control means for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

processing means for selectively processing said retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

11. (AMENDED) The system of claim 10, wherein **[said]** the storage means is an archive file.

12. (TWICE AMENDED) The system of claim 10, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage means, and further including

decompression means for decompressing **[said]** the compressed plurality of attributes and values in accordance with said control means retrieving **[said]** the compressed plurality of attributes and values.

13. (TWICE AMENDED) A method of validating a cryptographic policy file for controlling cryptographic functions in an application program, the method comprising **[the steps of]**:

retrieving a policy file including an attribute portion, a value portion and a signature portion from a storage means;

verifying a digital signature of an attribute-value pair stored in **[said]** the storage means;

performing a verification of **[said]** the application program version with a software-version attribute value of **[said]** the policy file in **[said]** the storage means; and

confirming localization information of **[said]** the application program with a localization in **[said]** the software-version attribute value of **[said]** the policy file.

14. (TWICE AMENDED) The method of claim 13, wherein **[said]** the policy file is determined invalid and ignored by **[said]** the application program when any one of **[said]** verifying, performing, and confirming **[steps]** fails.

15. (AMENDED) The method of claim 13, the method further **[including the step of]** comprising:

configuring each of **[said]** the application cryptographic capabilities in accordance with **[said]** the plurality of attribute-value pairs.

16. (AMENDED) The method of claim 13, wherein **[said step of]** verifying includes determining that one or a plurality of **[the]** certificates in **[said]** the digital signature certificate chain includes a certificate issued by a manufacturer of **[said]** the application.

17. (AMENDED) The method of claim 16, wherein **[said step of]** determining includes comparing **[said]** the digital signature to a predetermined certificate.

18. (AMENDED) The method of claim 17, wherein **[said]** the predetermined certificate includes a certification authority (CA) certificate.

19. (AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

a storage unit for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stores a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, **[said]** the signature portion including digital certificates for validating a signer's certificate;

a controller for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

a processor for selectively processing **[said]** the retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

20. (AMENDED) The system of claim 19, wherein each of **[said]** the cryptographic policy attributes includes an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression.

21. (AMENDED) The system of claim 20, wherein **[said]** the truth expression is one of a true flag, a false flag, and a conditional flag.

22. (AMENDED) The system of claim 21, wherein **[said]** the storage unit is an archive file.

23. (AMENDED) The system of claim 22, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompressing unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

24. (AMENDED) The system of claim 19, wherein **[said]** the storage unit is an archive file.

25. (AMENDED) The system of claim 24, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompressing unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

26. (AMENDED) The system of claim 19, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompressing unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

27. (AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

a storage unit for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stores a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, each of **[said]** the cryptographic policy attributes including an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression, and **[said]** the signature portion including digital certificates for validating a signer's certificate;

a controller for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and